UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/993,495 | 11/27/2001 | Doug Rollins | M4065.0486/P486 | 8165 |

24998 7590 10/06/2006

DICKSTEIN SHAPIRO LLP
1825 EYE STREET NW
Washington, DC 20006-5403

| EXAMINER | |
|---|---|
| GELAGAY, SHEWAYE | |
| ART UNIT | PAPER NUMBER |
| 2137 | |

DATE MAILED: 10/06/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/993,495 | ROLLINS, DOUG | |
| | Examiner | Art Unit | |
| | Shewaye Gelagay | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *07 September 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-12 and 14-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-12 and 14-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

# DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on September 7, 2006. Claims 1, 8, 14-15, 17 and 20 have been amended. Claims 1-12 and 14-26 are pending.

## *Response to Arguments*

2. Applicant's arguments filed on September 7, 2006 have been considered but are moot in view of the new ground(s) of rejection.

## *Claim Rejections - 35 USC § 112*

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 1 recites the limitation "said removed network communications device" in line 8. There is insufficient antecedent basis for this limitation in the claim.

## *Claim Rejections - 35 USC § 103*

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 6-8, 14-20 and 26 rejected under 35 U.S.C. 103(a) as being unpatentable over Serceki et al. (hereinafter Serceki) U.S. Publication Number 2003/0078072 in view of Lewis U.S. Patent Number 6,453,159.

As per claim 1:

Serceki teaches a method of updating an encryption key used by a wireless station for encrypted communications with a wired portion of the network, said method comprising:

physically separating from said wireless station a network communication device containing said encryption key; (Page 4, paragraphs 42-44)

connecting said removed network communications device to an encryption key updating device which is connected to a wired portion of said network said wired portion of said network containing an encryption key generator for providing a new encryption key to said updating device; (Page 3, paragraphs 32-33; page 4, paragraph 41)

replacing an existing encryption key in said network communications device with a new encryption key from said generator sent over said wired portion of said network; (Page 3, paragraph 33 and 35; Page 4, paragraph 43) and

physically reconnecting said network communications device containing said new encryption key with said wireless station of said network. (Page 3, paragraphs 33, 35; Page 4, paragraph 43)

In addition, Serceki further discloses a user is provided with a network device for physically exchanging encryption keys in a wireless network and network administrators create the device. (page 1, paragraph 8, page 3, paragraph 32) Furthermore, Serceki teaches the network

device can begin downloading updated keys at a company that may have several stations located through out the office space. (page 4, paragraphs 41-45)

Serceki does not explicitly disclose an encryption key which is accessed for use by said wireless station during said encrypted communications. Lewis in analogous art, however, discloses an encryption key which is accessed for use by said wireless station during used said encrypted communications.(figure 6, item 210; col. 12, lines 31-63) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Serceki with Lewis in order to avoid compromising the integrity of the network by preventing unauthorized access to the network. (col. 1, lines 7-9; Lewis)

As per claims 6-7, 14, 16 and 26:

The combination of Serceki and Lewis teaches all the subject matter as discussed above. In addition, Serceki further discloses a method wherein said network communications device is configured on a plug-in card and is physically connection to said network by inserting said network communications device into a card tray at said updating device. (Page 3, paragraph 31)

As per claims 8 and 15:

Serceki teaches a wireless network comprising:

a wired station connected to a wired network, (Page 4, paragraph 41) said wired station comprising:

an encryption key generator for generating an encryption key; (Page 3, paragraphs 32-33; page 4, paragraph 41)

a network communication device for transmitting said encryption key over said wired network; (Page 3, paragraph 31) and

a wired encryption key updating device connected to said wired network; (Page 3, paragraphs 32-33; page 4, paragraph 41)

a wireless station wirelessly connected to said network and communicating with said wired network through communications encrypted with an encryption key, (Page 4, paragraphs 42- 44) said wireless station comprising:

a wireless network communication device containing an encryption key, said wireless network communications device being physically disconnectable from said wireless station and physically connectable to an updating device wired to said network to receive and store as a new encryption key transmitted over said wired network by said wired network communications device. (Page 3, paragraph 33 and 35; Page 4, paragraph 43)

In addition, Serceki further discloses a user is provided with a network device for physically exchanging encryption keys in a wireless network and network administrators create the device. (page 1, paragraph 8, page 3, paragraph 32) Furthermore, Serceki teaches the network device can begin downloading updated keys at a company that may have several stations located through out the office space. (page 4, paragraphs 41-45)

Serceki does not explicitly disclose an encryption key which is accessed for use by said wireless station during said encrypted communications. Lewis in analogous art, however, discloses an encryption key which is accessed for use by said wireless station during used said encrypted communications.(figure 6, item 210; col. 12, lines 31-63) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Serceki with Lewis in order to avoid compromising the integrity of the network by preventing unauthorized access to the network. (col. 1, lines 7-9; Lewis)

As per claim 17:

Serceki teaches a wireless network communications device comprising:

A removable wireless communications network card adapted to be physically connected to and disconnected from a wireless station card interface; (Figure 3)

a storage area said network card which stores an updateable encryption key for use in conducting encrypted wireless network communications, (Figure 3, item 325) said encryption key being updateable when said card is connected to a wired network card interface which supplies a new encryption key. (Page 3, paragraph 33 and 35; Page 4, paragraph 42-43)

In addition, Serceki further discloses a user is provided with a network device for physically exchanging encryption keys in a wireless network and network administrators create the device. (page 1, paragraph 8, page 3, paragraph 32) Furthermore, Serceki teaches the network device can begin downloading updated keys at a company that may have several stations located through out the office space. (page 4, paragraphs 41-45)

Serceki does not explicitly disclose an encryption key for use by said wireless station when conducting encrypted communications. Lewis in analogous art, however, discloses an encryption key for use by said wireless station when conducting encrypted communications. (figure 6, item 210; col. 12, lines 31-63) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Serceki with Lewis in order to avoid compromising the integrity of the network by preventing unauthorized access to the network. (col. 1, lines 7-9; Lewis)

As per claims 18 and 19:

Serceki teaches all the subject matter as discussed above. In addition, Serceki further discloses a method wherein card interface for providing a new encryption key is a PCMCIA card interface. (Page 3, paragraphs 31-32)

As per claim 20:

Serceki teaches an encryption key programming system comprising:

an encryption key generator connected to a wired network; (Page 3, paragraphs 32-33; page 4, paragraph 41)

a programming device connected to said wired network for receiving over a wire connection an encryption key from said generator, said programming device being adapted to physically receive a wireless network communications device containing an updatable encryption key and storing said received encryption key in said wireless network communications device. (Page 3, paragraph 31-35; Page 4, paragraph 42-43)

In addition, Serceki further discloses a user is provided with a network device for physically exchanging encryption keys in a wireless network and network administrators create the device. (page 1, paragraph 8, page 3, paragraph 32) Furthermore, Serceki teaches the network device can begin downloading updated keys at a company that may have several stations located through out the office space. (page 4, paragraphs 41-45)

Serceki does not explicitly disclose an encryption key which is accessed for use by said wireless station during said encrypted communications. Lewis in analogous art, however, discloses an encryption key which is accessed for use by said wireless station during used said encrypted communications.(figure 6, item 210; col. 12, lines 31-63) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to

modify the method disclosed by Serceki with Lewis in order to avoid compromising the integrity of the network by preventing unauthorized access to the network. (col. 1, lines 7-9; Lewis)

7. Claims 2-3, 9-10 and 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Serceki et al. (hereinafter Serceki) U.S. Publication Number 2003/0078072 in view of Campbell, Jr. U.S. Patent 4,369,332.

As per claims 2-3, 9-10 and 21-23:

The combination of Serceki and Lewis teaches all the subject matter as discussed above. In addition, Serceki further discloses a network administrator decides to change security keys depending on internal policies at a regular intervals or after detecting a security breach. (Page 3, paragraph 41) Serceki does not explicitly disclose a method wherein said new encryption key is generated at user-defined intervals or on user-specified days. Campbell in analogous art, however, discloses a method wherein said new encryption key is generated at user-defined intervals or on user-specified days. Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Serceki with Campbell in order to provide a measure of added security for encryption keys while providing high level of convenience for users. (Page 1, paragraph 2 and 6; Serceki)

8. Claims 4-5, 11-12, 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Serceki et al. (hereinafter Serceki) U.S. Publication Number 2003/0078072 in view of Trieger United States Letter Patent Number 6,226,750.

As per claims 4, 11 and 24:

The combination of Serceki and Lewis teaches all the subject matter as discussed above. Both references do not explicitly disclose a method wherein said key generator generates a first

new encryption key; compares said new encryption key to the previous k encryption keys used in said network; and generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys.

Trieger in analogous art, however, discloses a method wherein said key generator generates a first new encryption key; (Col. 11, lines 30-32) compares said new encryption key to the previous k encryption keys used in said network; (Col. 11, lines 39-41) and generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys. (Col. 11, lines 38-43)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Serceki and Lewis to include wherein said key generator generates a first new encryption key; compares said new encryption key to the previous k encryption keys used in said network; and generates a second new encryption key if said first new encryption key matches any of said k previously used encryption keys. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Trieger (Col. 11, lines 38-39) in order to ensure the previous key is not reused.

As per claims 5, 12 and 25:

The combination of Serceki, Lewis and Trieger teaches all the subject matter as discussed above. In addition, Trieger further discloses a method wherein k is a user-defined number of previously used encryption keys. (Col. 11, lines 38-43)

***Conclusion***

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See Form PTO-892.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER